What is claimed is:

1. A digital content encryption apparatus of the digital content transmission system comprising:

a terminal unit having decryption algorithm, said terminal unit transmitting identity characters of a user and receiving and storing key information, said terminal unit receiving protocol including encrypted digital contents requested by the user and decrypting copyright protection protocol using the decryption algorithm and the key information to replay the digital contents, said key information formed to correspond to the identity characters; and

a service server having encryption algorithm, said service server generating the key information corresponding to the identity characters transmitted from the terminal unit and transmitting the key information to the terminal unit, said service server encrypting the digital contents using the key information and the encryption algorithm, said terminal unit transmitting to the copyright protection protocol to the terminal unit, said copyright protection protocol having a header and being formed by adding the encrypted digital contents to the header.

2. The apparatus of claim 1, wherein the terminal unit further comprises a user key and a temporary validation key, said user key being generated by the key information and key generation algorithm, said temporary validation key being decrypted by the user key, said encrypted digital contents included in the copyright protection protocol being decrypted by the temporary validation key.

3. The apparatus of claim 1, wherein the terminal unit comprises:

a first interface receiving the key information;

a use authority identifier identifying whether the user is authorized by comparing a hash value of the user key with a hash value set in user authorization information after reading the user authorization information of the header from the copyright protection protocol, the use authority identifier generating the user key by using the key

information;

a temporary validation key decryptor decrypting the temporary validation key using the user key; and

a digital content decryptor decrypting the encrypted digital contents using the temporary validation key decrypted by the temporary validation key decryptor.

4. The apparatus of claim 1, wherein the service server further comprises a user key and a temporary validation key, said user key being generated by the key information and key generation algorithm, said temporary validation key generated in response to the user's request being decrypted by the user key, said encrypted digital contents being decrypted by the temporary validation key.

5. The apparatus of claim 1, wherein said service server comprises:

a second interface receiving the identity characters input from the terminal unit;

key information generator generating the key information corresponding to the identity characters input from the second interface;

a user key generator generating the user key using the key information generated by the key information generator;

a temporary validation key generator generating the temporary validation key when the user accesses the service server through the second interface;

a user authorization information generator encrypting the temporary validation key using the user key generated by the user key generator to generate user authorization information;

a header generator generating the header using the user key, said header including the user authorization information; and

a protocol format generator generates the copyright protection protocol by adding the encrypted digital contents to the header generated by the header generator.

6. The apparatus of claim 1, further comprising:

a service sanction agent server receiving from the service server a signal con-

cerning digital content fees, said digital content fees caused by the transmission of the digital content requested by the user, said signal accumulating the digital content fees for the registered user's ID.

7. The apparatus of claim 1, wherein the terminal unit is connected to a public switched telephone network, said terminal unit having a network access program.

8. The apparatus of claim 1, wherein the terminal unit connected to a network, said terminal unit having a network access program.

9. The apparatus of claim 1, wherein the terminal unit is connected to a wireless network, said terminal unit having a network access program.

10. A digital content encryption apparatus of the digital content transmission system comprising:

a terminal unit having decryption algorithm, said terminal unit transmitting identity characters of a user and receiving and storing key information, said terminal unit receiving protocol including encrypted digital contents requested by the user and decrypting copyright protection protocol using the decryption algorithm and the key information to replay the digital contents, said key information formed to correspond to the identity characters;

a service server having encryption algorithm, said service server transmitting the key information to the terminal unit, said service server encrypting the digital contents using the key information and the encryption algorithm, said terminal unit transmitting to the copyright protection protocol to the terminal unit, said copyright protection protocol having a header and being formed by adding the encrypted digital contents to the header; and

a host server generating the key information corresponding to the identity characters transmitted from the service server and transmitting the key information to the service server, said host server storing the key information with the identity characters.

11. The apparatus of claim 10, wherein the terminal unit further comprises a user key and a temporary validation key, said user key being generated by the key information and key generation algorithm, said temporary validation key being decrypted by the user key, said encrypted digital contents included in the copyright protection protocol being decrypted by the temporary validation key.

12. The apparatus of claim 10, wherein the terminal unit comprises:

a first interface receiving the key information;

a use authority identifier identifying whether the user is authorized by comparing a hash value of the user key with a hash value set in user authorization information after reading the user authorization information of the header from the copyright protection protocol, the use authority identifier generating the user key by using the key information;

a temporary validation key decryptor decrypting the temporary validation key using the user key; and

a digital content decryptor decrypting the encrypted digital contents using the temporary validation key decrypted by the temporary validation key decryptor.

13. The apparatus of claim 10, wherein the service server further comprises a user key and a temporary validation key, said user key being generated by the key information and key generation algorithm, said temporary validation key generated in response to the user's request being decrypted by the user key, said encrypted digital contents being decrypted by the temporary validation key.

14. The apparatus of claim 10, wherein said service server comprises:

a second interface receiving the identity characters input from the terminal unit;

a user key generator generating the user key using the key information;

a temporary validation key generator generating the temporary validation key when the user accesses the service server through the second interface;

a user authorization information generator encrypting the temporary validation key using the user key generated by the user key generator to generate user authorization information;

a header generator generating the header using the user key, said header including the user authorization information; and

a protocol format generator generates the copyright protection protocol by adding the encrypted digital contents to the header generated by the header generator.

15. The apparatus of claim 10, wherein said host server comprises:

key information generator generating the key information corresponding to the identity characters input from the second interface.

16. The apparatus of claim 10, further comprising:

a service sanction agent server receiving from the service server a signal concerning digital content fees, said digital content fees caused by the transmission of the digital content requested by the user, said signal accumulating the digital content fees for the registered user's ID.

17. The apparatus of claim 10, wherein the terminal unit is connected to a public switched telephone network, said terminal unit having a network access program.

18. The apparatus of claim 10, wherein the terminal unit connected to a network, said terminal unit having a network access program.

19. The apparatus of claim 10, wherein the terminal unit is connected to a wireless network, said terminal unit having a network access program.

20. A digital content encryption apparatus of the digital content transmission system comprising:

a protocol format generator generating a copyright protection protocol, said

copyright protection protocol including a header and digital contents, said digital contents being encrypted, said header having information for decrypting and explaining the digital contents; and

a protocol format decoder having decryption algorithm, said protocol format decoder decrypting and replaying the digital contents according to the information of the header received from the protocol format generator.

21. The apparatus of claim 20, wherein the protocol format generator generates a user key by adding key information to key generation algorithm and calculates a hash value by adding the user key to hash algorithm, said protocol format generator encrypting a temporary validation key by using the user key, said header including user authorization information with the hash value and the encrypted temporary validation key, said key information being formed to correspond to identity characters of a user.

22. The apparatus of claim 20, wherein the protocol format decoder generates a user key by adding key information to key generation algorithm and decrypts a temporary validation key by using the user key, said protocol format decoder decrypting the encrypted digital contents with the temporary validation key, said key information being formed to correspond to identity characters of a user.

23. A digital content encryption apparatus of the digital content transmission system comprising a protocol format decoder for copyright protection, said protocol format decoder having decryption algorithm and receiving copyright protection protocol including encrypted digital contents, said protocol format decoder decrypting the copyright protection protocol using the decryption algorithm and key information to replay the encrypted digital contents.

24. The apparatus of claim 23, wherein the protocol format decoder generates a user key by adding key information to key generation algorithm and decrypts a temporary validation key from user authorization information by using the user key, said protocol for-

mat decoder decrypting the encrypted digital contents with the temporary validation key, said user authorization information being included in the copyright protection protocol.

25. A protocol for protecting copyright of digital contents including a header and the digital contents, said digital contents being encrypted, said header having information for decrypting the digital contents.

26. The protocol of claim 25, further comprising a field for indicating the size of the encrypted digital contents, and an additional information field.

27. The protocol of claim 25, wherein the header comprises a copyright support field for indicating whether the digital contents are under copyright protection, an unencrypted header field, and an encrypted header field.

28. The protocol of claim 25, wherein the header comprises a copyright support field for indicating whether the digital contents are under copyright protection, an unencrypted header field, a field for indicating the size of the unencrypted header field, an encrypted header field, a field for indicating the size of the encrypted header field.

29. The protocol of claim 27 or 28, wherein the unencrypted header field comprises a copyright library version field, a digital content conversion format field, a key generation algorithm field, a digital content encryption algorithm field, a field for indicating user authorization information at PC, and a field for indicating user authorization information at a replaying device.

30. The protocol of claim 29, wherein the field for indicating user authorization information at the PC and the field for indicating user authorization information at the replaying device comprise a field for indicating a hash value of the user key, and a field for indicating the size of the hash value generated by hash algorithm, a field for indi-

cating a resultant value of an encrypted temporary validation key, and a field for indicating the size of the resultant value of the encrypted temporary validation key, respectively.

31. The protocol of claim 27 or 28, wherein the unencrypted header field comprises a copyright library version field, a digital content conversion format field, a field for indicating the code of a digital content provider, a key generation algorithm field, a digital content encryption algorithm field, a field for indicating the number of users sharing PC, a field for indicating the number of users sharing a replaying device, a field for indicating user authorization information at the PC, and a field for indicating user authorization information at the replaying device.

32. The protocol of claim 31, wherein the field for indicating user authorization information at the PC and the field for indicating user authorization information at the replaying device comprise a field for indicating a hash value of the user key, and a field for indicating the size of the hash value generated by hash algorithm, a field for indicating a resultant value of an encrypted temporary validation key, and a field for indicating the size of the resultant value of the encrypted temporary validation key, respectively.

33. The protocol format of claim 27 or 28, wherein the encrypted header field comprises a field for encryption algorithm of the digital content, a field for indicating a basic process unit of the digital content, a field for indicating the number of encrypted byte, and a hash value field for a hash value for determining the state of the entire header.

34. A digital content encryption method of the digital content transmission system comprising the steps of:

a user inputting identity characters for membership registration through a terminal unit;

determining whether the user is registered by checking the input identity char-

acters;

storing information on the membership registration when the user is determined to be unregistered;

transmitting key information to the user in response to the user's request for digital contents;

determining whether a request signal for downloading digital contents;

encrypting the digital contents by a temporary validation key when the request signal is determined to be input from the user; and

transmitting the digital contents.

35. The method of claim 34 further comprising the step of transmitting information on the service fee to a service sanction agent server, said the information on the service fee being generated when the digital contents is transmitted to the user.

36. A method for generating user authorization information of digital contents comprising the steps of:

determining whether identity characters are received from a service server;

comparing the received identity characters with stored identity characters to determine whether identical identity characters with the received identity characters exist among the stored identity characters when the identity characters are received;

generating the key information when identical identity characters with the received identity characters is determined not to exist;

transmitting key information to the service server in response to the request of the service server; and

storing the user's identity characters with the transmitted key information.

37. A digital content encryption method of the digital content transmission system comprising the steps of:

receiving a request signal for digital contents from a user;

generating user authorization information using internally stored data when the

request signal is received;

generating a header having information on the digital contents and the user authorization information;

encrypting the digital contents; and

transmitting copyright protection protocol generated by adding the encrypted digital contents to the header.

38. The method of claim 37, wherein the internally stored data is key information generated correspondingly to the user's identity characters.

39. The method of claim 37, wherein the step of generating user authorization information further comprises:

generating a temporary validation key in response to the received request signal for the digital contents;

generating a user key using a key information; and

generating the encrypted user authorization information using the temporary validation key and the user key.

40. The method of claim 39, wherein the user authorization information comprises the encrypted temporary validation key and a hash value of the user key.

41. A method for encrypting digital content communication protocol comprising the steps of:

generating a temporary validation key when a user's request for the digital contents exists;

determining whether digital content encryption algorithm defined by a digital content provider exists;

generating a header according to the digital content encryption algorithm when the digital content encryption algorithm defined by the provider exists, and generating a header according to a basic algorithm when the digital content encryption algorithm de-

fined by the provider does not exist;

encrypting the digital contents after generating the header; and

adding the generated header to a front end of the digital contents.

42. The method of claim 41, further comprising the steps of:

determining whether additional information exists;

generating an additional information field when the additional information is determined to exist; and

adding the additional information field to a rear end of the digital contents.

43. The method of claim 41, wherein the step of generating the header comprises the step of:

generating copyright support information field and a field for indicating the size of an unencrypted header information and then adding them to the header;

adding the unencrypted header information field to the header;

generating user authorization information using a key information;

adding the generated user authorization information to the header;

generating header information for encrypting the digital contents;

encrypting the generated header information; and

adding an encrypted header information field and a field for indicating the size of the encrypted header information to the header.

44. The method of claim 43, wherein the step for generating the user authorization information comprises:

determining the existence of the key information or the temporary validation key;

using the key information to generate the user key when the key information and the temporary validation key are determined to exist;

calculating a hash value of the generated user key; and

encrypting the temporary validation key using the key encryption algorithm

and the generated user key after calculating the hash value.

45. A method for decrypting an encrypted digital contents comprising the steps of:

transmitting a digital content request signal to a service server;

receiving data and copyright protection protocol from the service server;

generating calculated data using internally stored data from the received data;

comparing the calculated data with data set in user authorization information included in the copyright protection protocol; and

confirming the use authority to decrypt the encrypted digital contents when the calculated data coincides with the data set in the user authorization information.

46. The method of claim 45, further comprising the step of decrypting and replaying the encrypted digital contents.

47. The method of claim 45, wherein the internally stored data are key information generated correspondingly to the user's identity characters.

48. The method of claim 45, wherein the user authorization information comprises a hash value of a user key generated by key information and an encrypted temporary validation key.

49. The method of claim 45, wherein the data set in the user authorization information is a hash value of a user key generated by key information.

50. The method of claim 45, wherein the calculated data are calculated by applying key information to key generation algorithm, a hash value being calculated from the calculated by hash algorithm, said calculated hash value being determined whether it is identical to a hash value set in the user authorization information, a temporary validation key included in the user authorization information being decrypted when said calculated hash value is determined to be identical to the set hash value, an encrypted header in-

cluded in the copyright protection protocol being decrypted the decrypted temporary validation key, said encrypted header being calculated into a hash value of a header using the hash algorithm, said key information being formed to corresponding to the user's identity characters.

51. The method of claim 50, wherein the calculated hash value of the header is determined whether it is identical to the hash value of a header set in the header, said encrypted temporary validation key being decrypted using the calculated data when the calculated hash value of the header is identical with the set header value of the header to confirm the use authority, said temporary validation key being replayed while decrypting the encrypted digital contents.

52. A method for receiving key information for user to be authorized to receive digital contents from a service server, comprising the steps of:

opening a screen for providing the digital contents via telecommunication;

requesting membership registration through the opened screen;

receiving key information corresponding to the membership registration; and

storing the received key information.

53. The method of claim 52, wherein the received key information is transmitted to an external slave device to be stored.

54. A method for receiving key information for user to be authorized to receive digital contents from a service server, comprising the steps of:

a processor opening a screen for providing the digital contents when a user inputs a key signal via an input device;

inputting request data on the open screen and transmitting it via the service server;

receiving the key information corresponding to the transmitted request data; and

storing the received key information.

55. The method of claim 54, wherein the request data are the user's identity characters.

56. The method of claim 54, wherein the key information received in the step of receiving the key information is transmitted to an external slave device to be stored.

57. A replaying device with decrypting function, comprising:

a memory storing an algorithm for decrypting protocol including encrypted digital contents, said memory further storing key information received when a user is a new member and the protocol received when the digital contents are requested;

a microcomputer storing the protocol inputted from an external device in the memory, and controlling output and encryption of the protocol according to the algorithm stored in the memory in accordance with a key signal received through a user key input unit; and

a decoder decoding the digital contents outputted from the microcomputer.

58. The replaying device of claim 57, wherein the decoder is a MPEG decoder.

59. The replaying device of claim 57, wherein the memory is a flash memory.

60. The replaying device of claim 57, wherein the microcomputer generates the user key through user authorization information of a received header by using the key information stored in the memory when the digital contents inputted according to the stored algorithm are encrypted, said microcomputer decrypting a temporary validation key included in the user authorization information of the header using the generated user key, said microcomputer decrypting and outputting the encrypted digital contents using a decrypted temporary validation key.

61. The replaying device of claim 57, wherein the microcomputer replays and outputs

the digital contents without decrypting them when the received digital contents are un-encrypted.

62. A digital content decrypting method of a replaying device with decrypting function, comprising the steps of:

receiving protocol comprising a header and encrypted digital contents, said header including user authorization information; and

storing the protocol in a record medium.

63. The method of claim 62, further comprising the step of decrypting and replaying the encrypted digital contents stored in the record media.

64. The method of claim 62, wherein the user authorization information comprises a hash value of a user key and an encrypted temporary validation key, said user key being generated by key information.

65. The method of claim 62, wherein the record medium is a flash memory.

66. A digital content decrypting method of a replaying device with decrypting function, comprising the steps of:

receiving encrypted digital contents and a header, said header having user authorization information;

generating calculated data using internally stored data after receiving the digital contents;

comparing the calculated data with the user authorization information;

decrypting the encrypted digital contents when the calculated data and the user authorization information are determined to be identical; and

replaying the decrypted digital contents.

67. The method of claim 66, wherein the calculated data are calculated by applying key

information to key generation algorithm,

a hash value being calculated from the calculated by hash algorithm,

said calculated hash value being determined whether it is identical to a hash value set in the user authorization information,

a temporary validation key included in the user authorization information being decrypted when said calculated hash value is determined to be identical to the set hash value,

an encrypted header included in the copyright protection protocol being decrypted the decrypted temporary validation key,

said encrypted header being calculated into a hash value of a header using the hash algorithm,

said key information being formed to corresponding to the user's identity characters,

said calculated hash value of the header being determined whether it is identical to the hash value of a header set in the header,

said encrypted temporary validation key being decrypted using the calculated data when the calculated hash value of the header is identical with the set header value of the header to confirm the use authority,

said temporary validation key being replayed while decrypting the encrypted digital contents.

68. The method of claim 66, wherein the internally stored data are key information generated correspondingly to user's identity characters.

69. A digital content decrypting method of a replaying device with decrypting function, comprising the steps of:

receiving key information and storing it on a record medium;

receiving encrypted digital contents and a header, said header having user authorization information;

generating a user key using the key information;

comparing a hash value of a user key set in the received user authorization information and a hash value of the generated user key; and

decrypting the encrypted digital contents when the hash value of the generated user key and the hash value of a user key set in the received user authorization information data are determined to be identical.

Add B1